Signature et preuve des envois dans le cadre des communications judiciaires électroniques

Montero, Etienne

Published in:
Phénix

Publication date:
2007

Document Version
le PDF de l'éditeur

CHAPITRE IV

SIGNATURE ET PREUVE DES ENVOIS DANS LE CADRE DES COMMUNICATIONS JUDICIAIRES ÉLECTRONIQUES

Étienne MONTERO
Professeur ordinaire aux
Facultés Universitaires Notre-Dame de la Paix

INTRODUCTION

1. Suivant le partage de la matière du présent ouvrage, il nous revient d'examiner trois questions choisies. La première concerne l'utilisation de la signature électronique dans le cadre des communications judiciaires électroniques (1). Il s'agit d'évaluer la pertinence des choix du législateur à cet égard (Section 1).

Comme l'on sait, le recours à l'envoi recommandé est fréquent dans la procédure judiciaire, cette forme de communication étant tantôt offerte, tantôt imposée par certaines dispositions du Code judiciaire. La second point que nous avons à traiter consiste à vérifier si le mécanisme de l'envoi recommandé et de son jumeau, le pli judiciaire, a été adéquatement transposé dans l'environnement électronique (Section 2).

Enfin, les dispositions légales relatives à la procédure par voie électronique mettent en scène un nouvel intervenant, le prestataire de services de communication. Pour certaines formes de communication, il est appelé à jouer un rôle important d'intermédiaire entre l'émetteur et le destinataire. Il y a lieu de cerner le statut juridique de cet acteur-pivot et de prendre la mesure de ses obligations et responsabilités (Section 3).

Section 1. – La signature électronique

2. De nombreuses dispositions du Code judiciaire et des textes régissant la procédure pénale imposent le recours à la signature. Dès lors que la procédure pourra dorénavant emprunter la forme électronique, il y avait lieu de permettre l'utilisation de certains procédés de signature électronique. À cet égard, la loi du 10 juillet 2006 aurait pu rester muette étant donné qu'un principe de non-discrimination a été posé, pour toutes matières, par l'article 4, § 5, de la loi du 9 juillet 2001. Autrement dit, il découle de cette disposition, de portée générale, qu'une signature électronique, quel que soit le procédé utilisé, ne peut être privée d'efficacité juridique au seul motif, notamment, que la signature se présente sous forme électronique (2). Néanmoins, le Roi

---

(1) Loi du 10 août 2005 instituant le système d'information Phenix, *M.B.*, 1er septembre 2005, p. 38305 ; Loi du 10 juillet 2006 relative à la procédure par voie électronique, *M.B.*, 7 septembre 2006, p. 45517 ; Loi du 5 août 2006 modifiant certaines dispositions du Code judiciaire en vue de la procédure par voie électronique, *M.B.*, 7 septembre 2006, p. 45527.

(2) Cf. l'article 4, § 5, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification » (*M.B.*, 29 septembre 2001, p. 33070), qui énonce d'autres motifs déclarés insuffisants, à eux seuls, pour priver une signature

est habilité à soumettre l'usage des signatures électroniques *dans le secteur public* à des exigences supplémentaires éventuelles, pourvu que celles-ci soient objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquent qu'aux caractéristiques spécifiques de l'application concernée (3). *A fortiori* le *législateur* pouvait-il subordonner l'efficacité juridique des signatures électroniques utilisées dans le cadre de la procédure judiciaire à des exigences supplémentaires. C'est le choix qui a été fait. À juste titre, il lui a paru opportun de limiter l'usage de la signature électronique à la signature dite « qualifiée ».

3. L'article 7 de la loi du 10 juillet 2006 s'énonce comme suit :

«Chaque fois qu'une disposition légale prévoit la signature d'une pièce de la procédure et qu'il s'agit d'une pièce électronique, celle-ci est pourvue de la signature qualifiée définie à l'article 2, 3°.

Cette signature qualifiée est assimilée à une signature manuscrite »

La signature qualifiée (4) s'entend de « *la signature électronique avancée définie à l'article 2, 2°, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, certifiée par un certificat qualifié visé à l'article 2, 4°, de cette loi et créée avec un dispositif sécurisé au sens de l'article 2, 7°, de cette loi* » (5).

Sans entrer dans une analyse approfondie des différents termes de cette définition, il n'est pas inutile d'en préciser un tant soit peu le sens et la portée. Ainsi, l'on entend par signature électronique avancée « *une donnée électronique, jointe ou liée logiquement à d'autres données électroniques servant de méthode d'authentification et satisfaisant aux exigences suivantes* :

a) être liée uniquement au signataire ;

b) permettre l'identification du signataire ;

électronique d'*efficacité juridique*. Cette dernière notion va au-delà de la simple recevabilité de toutes formes de signature électronique, contrairement à ce que laissent entendre les travaux préparatoires de la loi du 10 juillet 2006. Cf. Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 15.

(3) Article 4, § 3, de la loi du 9 juillet 2001.

(4) Jusqu'ici, l'expression « signature qualifiée » n'apparaissait dans aucun texte de loi, mais se trouvait sous la plume de certains auteurs pour désigner la signature visée à l'article 4, § 4, de la loi du 9 juillet 2001. Elle a été préférée à d'autres dénominations suggérées en doctrine au motif qu'elle utilise une terminologie figurant dans cette dernière loi (il y est question de 'certificat qualifié').

(5) Article 2, 3°, de la loi du 10 juillet 2006 relative à la procédure par voie électronique.

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable » (6).

On reconnaît dans cette définition la fonction d'identification (points a, b et c) et celle de maintien de l'intégrité du contenu de l'acte (point d). On remarque, par ailleurs, qu'il n'est pas fait mention de la fonction d'adhésion de la signature.

4. Par certificat, il faut entendre *« une attestation électronique qui lie des données afférentes à la vérification de signature* (7) *à une personne physique ou morale et confirme l'identité de cette personne »* (8), et par certificat qualifié *« un certificat qui satisfait aux exigences visées à l'annexe I de la loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la loi »* (9).

En substance, les exigences énoncées à l'annexe I concernent : l'identification du prestataire de service de certification (10), l'identification du signataire (11), les données permettant la vérification de signature (12), ainsi que certaines informations relatives au certificat lui-même et aux conditions particulières de son utilisation (13).

- S'il n'y a pas lieu de commenter outre mesure ces exigences, l'une d'entre elles mérite néanmoins quelques précisions. Dès lors que l'annexe I, point d), de la loi du 9 juillet 2001 prévoit que « tout certificat doit comporter la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire », le Conseil d'État était d'avis que l'avant-projet de loi devait faire de

(6) Article 2, 2°, de la loi du 9 juillet 2001.

(7) Soit, par ex., des codes ou des clés cryptographiques publiques, utilisés pour vérifier une signature électronique avancée. Cf. l'article 2, 8°, de la loi du 9 juillet 2001.

(8) Article 2, 3°, de la loi du 9 juillet 2001.

(9) Article 2, 4°, de la loi du 9 juillet 2001.

(10) Le certificat doit mentionner l'identité du prestataire de service de certification ainsi que le pays dans lequel il est établi (point b de l'annexe I) et être revêtu de sa signature électronique avancée (point h).

(11) Le certificat doit mentionner le nom du signataire (ou un pseudonyme) et éventuellement une qualité spécifique de ce dernier (points c et d).

(12) Le certificat doit comporter les « données afférentes à la vérification de signature » (entendez, dans la pratique actuelle, la clé publique du signataire) (point e).

(13) Le certificat doit comporter une mention indiquant qu'il est délivré à titre de certificat qualifié (point a), le code d'identité du certificat (point g), l'indication de la période de validité du certificat (point f), ainsi que les limites à son utilisation (points i et j).

cette faculté une obligation (14). Il n'a toutefois pas été suivi, le législateur estimant cette exigence « excessive et superflue » (15). En effet, le contrôle de la fonction affirmée par l'auteur de l'acte de procédure sera assuré grâce aux listes d'avocats, d'huissiers, de notaires et des membres de l'ordre judiciaire, qui seront mises à jour en permanence et accessibles à chacun par le biais d'Internet. Il est prévu, par ailleurs, qu'en cas de discordance entre la mention figurant sur un acte et ces listes, ces dernières l'emportent, sauf preuve contraire. Ces listes constituent dès lors la véritable source authentique de ce type d'information. Ainsi, en pratique, un greffier ne peut se fier à la qualité d'avocat indiquée dans un certificat ; il est tenu d'en vérifier la réalité directement dans les listes officielles. Il en ira de même en ce qui concerne l'identité et la qualité des greffiers ou des membres du ministère public : ils pourront s'identifier auprès du prestataire de service de communication au moyen de leur signature qualifiée ; en cas de doute, il appartiendra à ce dernier de consulter la liste des membres de l'ordre judiciaire qui est prévue par l'article 12 de la loi du 5 août 2006, insérant un nouvel article 315*bis* dans le Code judiciaire. En définitive, le destinataire sera toujours en mesure de vérifier l'identité de la personne qui lui adresse un acte (soit par le biais de la signature électronique, soit sur foi de l'affirmation du prestataire de service de communication), de même que sa qualité professionnelle (par la consultation des listes électroniques).

5. Pour être qualifié, le certificat doit en outre être délivré par un prestataire satisfaisant aux exigences de l'annexe II. Celles-ci concernent l'aptitude du prestataire à fournir, dans des conditions optimales, des services de certification (16) : solidité financière (17), qualification du personnel (18), utilisation de systèmes et de produits fiables et suffisamment sécurisés (19), capacité d'assurer le fonctionnement d'un service d'annuaire et de révocation rapide et sûr (20), etc.

---

(14) Projet de loi relatif à la procédure par voie électronique, Avis du Conseil d'État n° 37.942/2 donné le 13 janvier 2005, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 88.

(15) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 11.

(16) Cf. Annexe II, point a, d, i, j et k.

(17) Annexe II, point h.

(18) Annexe II, point e.

(19) Annexe II, points f, g et l.

(20) Annexe II, points b et c.

6. Enfin, l'expression « dispositif sécurisé (de création de signature) » désigne tout « *dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature* (21) *qui satisfait aux exigences de l'annexe III de la loi* » (22). Ces exigences visent à assurer que les données utilisées pour la création de la signature (entendez : la clé privée) soient uniques et que leur confidentialité soit suffisamment protégée contre l'usurpation par des tiers ou le déchiffrement frauduleux au départ de la clé publique. Il est exigé également que les dispositifs sécurisés de création de signature ne modifient pas les données à signer et n'empêchent pas que celles-ci soient soumises au signataire avant le processus de signature.

7. Que retenir de l'ensemble de ces exigences techniques ? Tout simplement, ceci : la réunion de ces trois exigences fondamentales – signature électronique avancée, certificat qualifié et dispositif sécurisé de création de signature – caractérise les formes de signature électronique qui présentent le plus haut degré de sécurité. En d'autres termes, parmi les différents procédés de signature électronique disponibles, c'est la signature qualifiée qui a été retenue en matière d'actes de procédure. Le législateur a ainsi fait le choix de la sécurité maximale sur le plan technique (§ 1) et juridique (§ 2).

§ 1. Le choix de la fiabilité technique

8. La procédure judiciaire nécessite des procédés conduisant à une authentification irréprochable, limitant au maximum les possibilités de contestation relative à l'identité des signataires et garantissant le maintien de l'intégrité des documents signés (23). Le projet Phenix – le mesure-t-on assez ? – est un projet d'envergure, aussi audacieux que périlleux à mettre en œuvre. On comprend que le législateur ait voulu prendre un maximum de précautions pour un minimum de risques en termes de sécurité du système, notamment en ce qui concerne la fiabilité des signatures électroniques. Aussi a-t-il été sage d'autoriser une seule forme de signature électronique, la plus sûre actuellement et la moins susceptible de contestation, à savoir la signature qualifiée.

Les différentes définitions reproduites ci-dessus se veulent neutres sur le plan technologique. Ainsi, il n'est pas question de « clés privées » ou de « clés publiques », mais de « données afférentes à la création de

(21) Soit des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique avancée. Cf. l'article 2, 6°, de la loi du 9 juillet 2001.

(22) Article. 2, 7°, de la loi du 9 juillet 2001.

(23) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 15.

signature » et de « données afférentes à la vérification de signature ». Mais, il est évident que les rédacteurs de la loi du 9 juillet 2001 ont constamment eu présent à l'esprit un modèle mental précis : la signature numérique à clés cryptographiques asymétriques certifiées. Dans l'état actuel de la technique et en pratique, cette forme de signature électronique, qui répond aux conditions de la signature qualifiée, est sans conteste la plus apte à remplir les fonctions traditionnellement dévolues à la signature : permettre l'identification du signataire et attester son adhésion au contenu de l'acte. Elle est également la plus apte à garantir le maintien de l'intégrité du contenu de l'acte.

Bref, la signature qualifiée présente le plus haut degré de fiabilité. Pour s'en convaincre, il nous est apparu utile d'en décrire brièvement le fonctionnement. Les explications qui suivent nous ont semblé d'autant plus opportunes que la signature numérique est, logiquement, encore peu connue d'un certain nombre d'acteurs du monde judiciaire. Il va de soi que le lecteur averti peut passer directement au paragraphe 2.

A. – La signature numérique – Théorie et pratique

9. En substance, la signature numérique est fondée sur les procédés de cryptographie, qui combine l'utilisation d'un algorithme et d'une (ou deux) clé(s) de chiffrement. Cette dernière opération consiste en la transformation d'un message dit « en clair » en une chaîne de caractères alphanumériques qui ne sont compréhensibles que pour la personne autorisée. Le chiffrement, est généralement réalisé à l'aide de produits qui, pour la plupart, sont fondés sur le *Data Encryption Standard* (DES). Il s'agit d'un système cryptographique à clé unique (ou clé secrète) utilisant un algorithme qui, comme le suggère son nom, chiffre et déchiffre un message à l'aide d'une seule clé. Un tel procédé est surtout efficace dans les réseaux fermés. La nécessité de faire connaître la clé à son destinataire, avec les inévitables risques d'interception, entraîne qu'à lui seul, il est, en revanche, inadapté aux réseaux ouverts, singulièrement pour une utilisation à des fins de signature.

Le problème du partage des clés a été résolu par le développement de la cryptographie asymétrique, dite aussi « à clé publique ». Le mécanisme repose sur l'utilisation d'une paire de clés complémentaires : une clé privée (ou secrète) et une clé publique, qui est une fonction mathématique irréversible de la clé privée (24). L'application la plus

(24) Cela signifie que la clé publique est générée à partir de la clé privée, mais qu'il est impossible, en principe (c'est-à-dire dans un temps et avec des moyens matériels, humains et financiers

répandue de cryptographie à clé publique est le R.S.A., du nom de ses concepteurs (Rivest, Shamir et Adleman, du M.I.T.).

En réalité, les clés ne sont généralement pas appliquées sur l'ensemble du message ou du document à signer mais, plus précisément, sur un condensé ou empreinte du message (ou document). Cette empreinte est une version extrêmement réduite de l'information, obtenue à l'aide d'une fonction mathématique dite de « hachage » (25). L'intérêt de l'empreinte est multiple : elle permet non seulement des gains de temps considérables (26) mais aussi une vérification de l'intégrité des données (27).

10. Pratiquement, pour signer un message (ou document), son auteur génère une empreinte de celui-ci et y applique sa clé privée. Ensuite, il expédie tant le message complet « en clair » (28) que l'empreinte signée au destinataire. Ce dernier peut procéder à la vérification de signature en appliquant à l'empreinte du message la clé publique de l'émetteur (laquelle est complémentaire à sa clé privée). Si l'opération de vérification réussit, le destinataire est assuré que le document (ou le message) émane bien de son auteur dûment identifié (29). Enfin, il applique la fonction de hachage au message complet, et compare l'empreinte générée avec l'empreinte qu'il vient de décrypter (30). Si elles sont identiques, il a la certitude que le message n'a pas été modifié et que ce qu'il a lu en clair correspond bien au contenu auquel l'émetteur a appliqué la fonction de hachage et sa clé privée. Dans le cas contraire, il sait que le message a été modifié par un tiers ou altéré lors de sa transmission.

---

raisonnables) de découvrir la clé privée au départ de la clé publique (déchiffrement de cette dernière par cryptanalyse).

(25) D'où le terme anglais de *hash* très couramment employé pour désigner l'empreinte.

(26) En effet, les opérations de cryptage mobilisent d'importantes ressources informatiques : le cryptage et le décryptage demandent un certain temps d'exécution ; celui-ci est fonction de la taille des données cryptées. Or, l'empreinte est, par définition, un condensé de l'information de départ, de taille largement inférieure ; sa manipulation cryptographique est donc beaucoup plus aisée.

(27) En effet, les algorithmes de hachage sont conçus en manière telle qu'il est très difficile de générer deux empreintes identiques à partir de deux messages différents.

(28) L'expéditeur procédera inversement s'il entend assurer la confidentialité de la communication. Concrètement, il chiffrera le message à l'aide de la clé publique du destinataire, qui pourra le déchiffrer uniquement au moyen de sa propre clé privée (complémentaire à sa clé publique). Étant, par hypothèse, détenteur unique de sa clé privée, il sera le seul à pouvoir prendre connaissance du message. Les deux fonctions peuvent être combinées pour l'envoi de documents ou de messages à la fois signés et confidentiels.

(29) Pourvu qu'un certificat délivré par une autorité de certification confirme que la clé publique appartient effectivement à l'émetteur.

(30) Il va de soi que toutes les opérations décrites ci-dessus sont réalisées par le logiciel de signature de l'intéressé.

L'utilisation de la signature numérique fondée sur un cryptosystème asymétrique garantit de surcroît le maintien de l'intégrité du message expédié et fait obstacle aux velléités de répudiation de ce dernier par son auteur (31).

B. – Le rôle des certificats

11. La fiabilité du procédé de signature numérique suppose l'instauration d'un mécanisme de contrôle visant à s'assurer que les clés cryptographiques correspondent bien aux personnes qui s'en prétendent titulaires. En effet, la technologie de la cryptographie asymétrique garantit que des données que l'on peut décrypter à l'aide d'une clé publique ont bien été chiffrées à l'aide de la clé privée correspondante. Toutefois, si le destinataire du message ne connaît pas l'expéditeur ou est en contact électronique avec lui pour la première fois, rien ne lui garantit que l'expéditeur est bien la personne qu'elle prétend être. D'où le recours aux certificats. Concrètement, un tiers garantit l'identité du titulaire d'une clé publique, sous la forme d'une attestation électronique contenant en principe la clé publique et la mention de l'identité de son titulaire (32), une date d'expiration, et l'adresse d'une liste de révocation qui permettra de vérifier, généralement en ligne, si le certificat n'a pas été révoqué. Enfin, le certificat est lui-même signé par le tiers (*supra*, n° 4).

12. Le système dépend naturellement de la confiance que l'on accorde au tiers. Celle-ci est tributaire du schéma de confiance employé. Il en existe deux principaux : l'infrastructure à clé publique classique (*Public Key Infrastructure* ou *PKI*) et la méthode du *Web of Trust* (33). On se borne à décrire le système de l'infrastructure à clé publique, qui correspond au choix du législateur dans le projet Phenix.

C. – Les infrastructures à clé publique

13. Ce système est le plus couramment utilisé sur le marché professionnel. Il repose sur l'intervention d'un tiers de confiance, appelé

---

(31) Voy. D. Gobert et E. Montero, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *D.A./O.R.*, n° 53, 2000, pp. 17 et s., spéc. pp. 20 à 24.

(32) Ainsi que d'éventuelles mentions supplémentaires telles qu'adresse, profession, date de naissance…

(33) Dans ce schéma, la confiance n'émane plus tant de la qualité des personnes qui vérifient l'identité des titulaires de clés publiques que de leur nombre. *Thawte* est paradigmatique à cet égard. Cette entreprise délivre un certificat pour ainsi dire vide : pour avoir son nom inscrit dans le certificat, l'intéressé doit faire vérifier son identité, à la faveur de rencontres individuelles avec une série de personnes ayant déjà obtenu des certificats Thawte, jusqu'à totaliser 50 points de confiance (*trust points*). Le système de *trust points* permet une évaluation fine de la confiance que l'on peut accorder à un certificat et établit une échelle là où un système de *PKI* classique est binaire : une paire de clés est certifiée ou non.

prestataire de service de certification (34). Sa mission est double : d'une part, vérifier l'identité des titulaires de clé publique et générer les certificats, d'autre part, organiser la publicité la plus large des certificats émis. Le tiers certificateur est également tenu de maintenir à jour le répertoire contenant les certificats de clé publique, en veillant, au besoin, à leur révocation, à leur suspension ou à leur renouvellement.

Préalablement à l'émission du certificat, le tiers vérifie donc l'identité et, le cas échéant, la qualité (titre, fonction...) du candidat au certificat. Cette étape a pour nom « l'enregistrement ».

La fonction d'enregistrement peut être réalisée par l'autorité de certification elle-même ou déléguée par cette dernière à un tiers (35). Il est évident que la confiance que l'on peut accorder à l'autorité d'enregistrement est cruciale pour le bon fonctionnement du système puisque c'est elle qui effectue les vérifications d'identité « *face-to-face* ». Cependant, les destinataires des documents signés ne connaissent, grâce au certificat, que le prestataire des services de certification, qui est tenu de répondre des éventuelles défaillances de l'autorité d'enregistrement.

D. – Qu'en est-il de la fonction de signature de la carte d'identité électronique ?

14. Dans son avis sur l'avant-projet de loi relatif à la procédure par voie électronique, le Conseil d'Etat s'interroge sur le lien existant entre la signature qualifiée et la signature électronique figurant sur la carte d'identité électronique (CIE) de la personne (36). La question est pertinente vu que, dans l'intention du législateur, la CIE constituera un des mécanismes d'identification au sein du système Phenix (37).

En réalité, la CIE met en œuvre une signature numérique à double clé cryptographique, fondée sur la technologie RSA, et une infrastructure à clé publique. Elle répond incontestablement aux conditions de

---

(34) Cf. la loi du 9 juillet 2001 « fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification » (*M.B.*, 29 juillet 2001, p. 33070).

(35) On notera aussi l'existence de chaînes de confiance : une autorité de certification telle que VERISIGN se contente de certifier la signature d'une entreprise, et cette dernière prend alors le relais et devient l'autorité d'enregistrement et de certification de ses employés. Elle émet donc les certificats couvrant la signature de ses employés. Ce type de pratique est généralement optionnelle : l'entreprise peut devenir sa propre autorité de certification si elle le souhaite.

(36) Projet de loi relatif à la procédure par voie électronique, Avis du Conseil d'État n° 37.942/2 donné le 13 janvier 2005, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 89.

(37) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 12.

la signature qualifiée et bénéficie dès lors du principe d'assimilation de plein droit à la signature manuscrite.

15. Sans entrer dans une analyse approfondie de la CIE (38), soulignons toutefois, au passage, la triple fonction offerte par celle-ci. Elle permet, tout d'abord, la classique identification physique de la personne, grâce aux données visibles à l'œil nu figurant sur la carte. La nouveauté vient des données figurant sur la puce (39), lisibles de manière électronique à l'aide d'un microprocesseur, qui permettent de remplir une fonction d'authentification (électronique) et de signature (électronique). Une certaine confusion entoure parfois ces deux fonctions distinctes.

16. La fonction d'*authentification* consiste en un processus actif par lequel le titulaire de la carte s'identifie de façon électronique afin de prouver avec certitude qu'il est effectivement celui qu'il prétend être. Pratiquement, l'intéressé insère la carte dans un terminal *ad hoc* et forme un code secret (qu'il est seul censé connaître). L'insertion de ce code PIN permet de déverrouiller la clé privée présente sur la CIE qui, à son tour, génère un message codé. En fait, pareil cryptogramme résulte du chiffrement d'un 'nombre', produit de manière dynamique par la carte, lors de chaque insertion du code PIN (40). Envoyé par le terminal au destinataire, il authentifie l'identité du titulaire (par exemple auprès d'un site web).

Dans le mécanisme de *signature*, ce n'est pas un 'nombre', créé aléatoirement par la carte, qui est crypté au moyen de la clé privée du titulaire, mais un 'message doté d'un contenu sémantique' (tel un acte de procédure, en l'occurrence). L'intérêt n'est plus seulement d'authentifier le titulaire, mais aussi d'attester son adhésion à un contenu. Pour le reste, le processus se déroule de façon similaire (41).

---

(38) Pour de plus amples développements, O. Goffard et E. Roger France, « L'introduction de la carte d'identité électronique en droit belge par la loi du 25 mars 2003 : aspects juridiques », in *Aspects juridiques du paiement électronique – Juridische aspecten van de elektronische betaling*, tome 2, Bruxelles, Kluwer, 2004, pp. 123 et s.

(39) Sur la puce figurent des informations concernant : 1° les clés d'identité et de signature, 2° les certificats d'identité et de signature, 3° le prestataire de service de certification accrédité, 4° la résidence principale du titulaire, etc. Le titulaire peut renoncer à l'activation des données visées aux points 1° à 3°. Cf. l'article 14 de la loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.*, 28 mars 2003, p. 15.921.

(40) Le cryptogramme est aléatoirement différent lors de chaque insertion du code PIN, ce qui représente une sécurité supplémentaire.

(41) Le titulaire insère la carte dans le terminal et introduit son code secret. Comme expliqué plus haut (*supra*, n° 9), le message est transformé en une suite de symboles (fonction de hachage). Par activation de la clé secrète, le condensé ainsi obtenu est chiffré de manière à générer le cryptogramme de signature. Toute cette phase se déroule entièrement dans la carte. La vérification de la

§ 2. Le choix de la sécurité juridique

17. Parmi les mécanismes de signature électronique, la signature qualifiée apparaît aussi comme le plus sûr pour des motifs juridiques.

La signature qualifiée bénéficie d'un régime de faveur : à la différence des autres procédés de signature électronique, elle est assimilée *de plein droit* à la signature manuscrite. Ce principe d'équivalence est consacré à l'article 7, alinéa 2, de la loi du 10 juillet 2006. Il s'en suit qu'*a priori*, la signature qualifiée ne devrait pas donner plus de soucis que la signature manuscrite.

18. Même si ce n'est pas courant, il peut arriver que la signature manuscrite fasse l'objet d'une contestation. Pratiquement, le débat judiciaire peut tourner autour de deux questions distinctes (42). Une première question concerne la validité de la signature. En cas de signature valable, une seconde question peut surgir : cette signature est-elle imputable au signataire apparent ? Il est encore loisible à ce dernier de désavouer son écriture, auquel cas, selon le contexte, le signataire apparent peut soit inciter le demandeur à recourir à la procédure de vérification d'écritures, soit engager une procédure d'inscription de faux.

La signature électronique peut donner lieu au même double débat.

A. – Question de validité de la signature

19. Tout d'abord, le juge peut être invité à se prononcer sur la validité d'une signature.

En matière de signature traditionnelle, ce simple problème juridique de qualification peut être aisément tranché par le juge. Ainsi peut-il estimer que tel signe ne constitue pas une signature valable pour divers motifs : soit le signe est illisible; soit il n'a pas été apposé directement sur l'acte mais par le truchement d'un papier carbone, d'une photocopie ou d'une télécopie…; soit il ne manifeste pas l'adhésion de son auteur au contenu de l'acte (eu égard à son emplacement…).

20. Le même type de contestation peut s'élever à propos d'une signature électronique.

---

signature se fait par application de la clé publique que le terminal se procure auprès du prestataire de service de certification. Pratiquement, la clé publique permet de décoder le cryptogramme de signature et de le transformer, à son tour, en une suite de symboles. Le terminal compare alors les symboles obtenus à ceux qu'il a lui-même produits : si les condensés sont identiques, la vérification est concluante et la signature considérée valide. Cette phase de vérification de signature se déroule entièrement au sein du terminal.

(42) À cet égard, D. MOUGENOT, *La preuve*, 3e éd., Bruxelles, Larcier, 2002, p. 225, n° 158-1 ; E. MONTERO, « L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique fonctionnaliste ? », *Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, pp. 179-210, spéc. pp. 194 et s.

C'est ici que s'apprécie tout l'intérêt d'imposer, pour les actes de procédure, le recours à la signature qualifiée. En effet, la signature qualifiée est assimilée automatiquement à une signature manuscrite : « le juge n'est dès lors pas tenu de procéder à d'autres vérifications que celles qu'il effectuerait en présence d'une signature manuscrite » (43). En réalité, ces deux types de signature se présentant sous des dehors assez différents, les vérifications qui s'imposent ne sont pas comparables pratiquement. Mais il est vrai, que, dans le cas de la signature qualifiée, elles seront aussi *simples* et *objectives* qu'en matière de signature manuscrite. Si la signature (présentée comme qualifiée) est certifiée par un prestataire *accrédité*, le juge pourra se borner à constater cette accréditation (laquelle *suppose* le respect des exigences des annexes I, II et III de la loi du 9 juillet 2001). Si la signature est délivrée par une autorité de certification *non accréditée*, le respect des exigences énoncées dans les trois annexes de la loi devrait être démontré ; toutefois, en pratique, les vérifications à effectuer restent relativement aisées (44).

En revanche, le débat portant sur la validité d'une signature électronique ordinaire, voire avancée (45), conduit à des vérifications plus *complexes* et *subjectives*. En effet, le juge doit contrôler si le procédé de signature électronique qui lui est présenté remplit les fonctions traditionnellement dévolues à la signature. Pratiquement, il lui revient d'apprécier l'aptitude du procédé à identifier le signataire et à attester son adhésion au contenu de l'acte. À cet égard, il jouit d'un incontestable pouvoir d'appréciation quant au degré de fiabilité dont il se satisfait. Pourvu qu'il motive sa décision de façon cohérente, on conviendra que sa marge de manœuvre est appréciable à l'heure de considérer si le procédé est valable ou non.

Aussi, à la différence des signatures tant manuscrites que qualifiées, les signatures électroniques visées à l'article 2, 1° et 2°, de la loi du 9 juillet 2001 risquent de donner du fil à retordre sur le terrain de la qualification.

---

(43) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 16.

(44) Il suffira au juge de vérifier que le certificat est qualifié et de demander une attestation à l'administration chargée de contrôler ces prestataires. En ce sens, L. Lecocq et B. Vanbrabant, « La preuve du contrat conclu par voie électronique », in *Le commerce électronique : un nouveau mode de contracter ?*, Liège, Éditions du Jeune Barreau, 2001, p. 119-121, n^{os} 106 et 107; M.E. Storme, « De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen », *R.W.*, 2000-2001, p. 1519, n° 45; L. Guinotte, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, p. 558.

(45) Article 2, 1° et 2°, de la loi du 9 juillet 2001.

21. *En pratique*, la signature manuscrite réserve normalement peu de surprise : pourvu qu'elle consiste en la marque habituelle du signataire et qu'elle soit tracée au bon endroit, sa validité est assurée. Sauf rares exceptions (la griffe, les empreintes digitales, la signature à main guidée…), on n'a, du reste, jamais eu à se préoccuper de la fiabilité de la signature sur papier, ni du procédé utilisé. Le juge peut, du reste, trancher seul et aisément la question de la qualification.

Les signatures électroniques sont nettement plus imprévisibles. Hors la signature qualifiée, l'on a vu qu'en cas de contestation, il y a lieu de convaincre le juge que le mécanisme utilisé remplit effectivement les fonctions classiques de la signature. Force est d'admettre que la liberté d'appréciation laissée au juge à cet égard entraîne une insécurité juridique, qui est pratiquement négligeable en présence d'une signature traditionnelle… ou qualifiée. En outre, il devra souvent faire appel à un expert pour évaluer la validité d'un procédé de signature électronique qui ne répond pas aux critères de la signature qualifiée. On sait les inconvénients qui s'ensuivent en termes de coût et d'allongement des délais de procédure.

22. Au total, le législateur a eu raison de couper court à toutes ces discussions en imposant le recours à la seule signature qualifiée en matière d'actes de procédure. On ne peut que l'approuver sur ce point. Comme le relèvent avec raison les auteurs du projet devenu la loi du 10 juillet 2006 (46), on ne se situe plus ici dans le cadre du droit civil de la preuve, dans lequel le juge ne peut soulever d'office une contestation : saisi d'un problème de preuve, il ne peut d'initiative vérifier la validité d'une signature si les parties ne l'y invitent pas dans leurs conclusions. En revanche, beaucoup de règles de procédure touchant à l'ordre public, le juge est tenu de contrôler la régularité des actes de procédure accomplis : s'ils sont porteurs d'une signature électronique, il est donc tenu de vérifier si celle-ci est valable. Comme on l'a vu, la signature qualifiée – et elle seule – garantit que cette vérification puisse être opérée, par le tribunal, de manière simple et rapide.

B. – Question d'imputabilité de la signature

23. De manière générale, lorsqu'une signature est estimée valable, le prétendu signataire peut encore dénier sa signature et, selon le

(46) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 16.

contexte, soit demander l'inscription de faux (47), soit obliger la partie qui invoque l'acte à demander une vérification d'écritures (48).

À ce propos, les travaux préparatoires de la loi du 10 juillet 2006 affirment reprendre de « manière identique» le principe d'équivalence inscrit à l'article 4, § 4, de la loi du 9 juillet 2001. Ce n'est pas rigoureusement exact. En effet, l'article 4, § 4, *initio*, réserve *explicitement* la possibilité de désavouer une signature électronique présentée comme qualifiée. Cette disposition est libellé comme suit : *« Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilé à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale ».*

24. Pourquoi ne pas s'être contenté d'un simple renvoi à l'article 4, § 4 ? Cette légère différence prête-t-elle à conséquences ? À vrai dire, non. L'absence de référence aux articles 1323 et suivants du Code civil est évidemment pertinente. La vérification d'écritures est propre à l'acte sous seing privé. Ces dispositions sont donc étrangères à la procédure judiciaire. Qui plus est, la plupart des actes de procédure requérant une signature qualifiée doivent être accomplis par des officiers publics : magistrats, greffiers...(49) Aussi s'analysent-ils en des actes authentiques. À ce titre, ils font foi par eux-mêmes de l'écriture de ceux dont ils émanent, jusqu'à inscription de faux. Cela étant, d'autres actes (déclarations, requêtes, rapports d'expertise...) doivent revêtir la signature qualifiée, respectivement de la partie concernée, de la partie lésée, du requérant ou de son avocat, de l'expert...(50)

Est-il imaginable qu'une personne pose un acte de procédure sous l'identité d'une autre ?

Certes, on ne peut exclure totalement qu'une personne perde la maîtrise de sa clé privée. À cet égard, deux hypothèses sont généralement évoquées : l'usurpation ou la perte du support sur lequel elle est enregistrée (carte à puce, CIE...) et le déchiffrement frauduleux par cryptanalyse. Néanmoins, dans le premier cas de figure, l'intéressé

---

(47) La procédure d'inscription de faux civil est décrite aux articles 895 et suivants du Code judiciaire. La demande d'inscription en faux civil est communicable au ministère public (C. jud., art. 764, 5°).

(48) La procédure de vérification d'écritures est décrite aux articles 883 et suivants du Code judiciaire.

(49) Loi du 10 juillet 2006, art. 31, § 1er, art. 34, § 1er, art. 36, § 2, etc.

(50) Loi du 10 juillet 2006, art. 34, § 4, art. 34, § 6, etc.

peut au plus vite demander la révocation de son certificat (51), ce qui limite le risque d'une utilisation de sa clé privée à son insu. Quant au second cas de figure envisageable, il est infiniment marginal.

En toute hypothèse, si d'aventure une éventualité de ce genre devait se produire, une procédure d'inscription de faux pourrait être engagée. En réalité, on voit mal qui aurait intérêt a accomplir un acte de procédure sous une fausse identité, s'exposant au demeurant à l'incrimination de faux en informatique (52).

25. En conclusion, on se félicite que le législateur ait choisi d'imposer le recours à la seule signature qualifiée en matière d'actes de procédure. Il s'agit du procédé de signature électronique le plus fiable sur le plan technique et juridique. Elle expose à peu de soucis tant au niveau de sa validité que de son imputabilité. De plus, le procédé de signature implémenté dans la carte d'identité électronique répond sans conteste aux critères de la signature qualifiée.

SECTION 2. – LA COMMUNICATION JUDICIAIRE PAR ENVOI RECOMMANDÉ ET PLI JUDICIAIRE ÉLECTRONIQUES

26. Le recours à l'envoi recommandé est fréquent dans les communications judiciaires (53). Ainsi, certaines communications adressées à un magistrat ou un greffier (dépôt d'un acte de procédure ou simple communication) doivent (54) ou peuvent (55) avoir lieu par pli recommandé. En sens inverse, diverses dispositions du Code judiciaire prévoient que le ministère public ou le greffier s'adresse aux justiciables en faisant procéder à des notifications par pli judiciaire. Certaines dispositions imposent également la notification par pli recommandé avec accusé de réception (56).

Désormais, ces modes de communication – recommandé et pli judiciaire – peuvent emprunter la voie électronique. En réalité, le pli judiciaire s'apparente à une forme d'envoi recommandé avec accusé de ré-

(51) Cf. loi du 9 juillet 2001, article 12, § 1er, 13 et 19. En cas de perte ou vol de la carte d'identité électronique, cf. l'art. 16 de la loi du 25 mars 2003 et l'article 7 de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité (*M.B.*, 28 mars 2003, p. 15929).

(52) C. pén., art. 210*bis*.

(53) Cf. la contribution de D. MOUGENOT.

(54) Certains types de requête.

(55) Envoi de conclusions, requêtes ou autres actes généralement quelconques.

(56) Par exemples, les articles 1275, 1303, 1339, 1457 et 1627.

ception. C'est pourquoi nous envisagerons conjointement ces deux procédés (57).

Dans les lignes qui suivent, on se propose de présenter les textes qui forment le siège de la matière (§ 1), avant de livrer une analyse critique de la manière dont le procédé a été transposé dans l'environnement électronique (§ 2).

§ 1. D'une réforme à l'autre

27. La reconnaissance des formes électroniques du recommandé dans la procédure judiciaire s'est faite en deux temps (58). Les dispositions de droit judiciaire de la loi du 20 octobre 2000 contenaient quelques règles, très parcellaires, relatives à la communication judiciaire. Les deux lois de 2006 sont plus ambitieuses puisqu'elles embrassent l'ensemble de la communication judiciaire.

A. – Acte I : une réforme timide et boiteuse

28. On se rappellera que l'admission du recommandé électronique dans les communications judiciaires a été envisagée dès l'année 2000. Cette première tentative de réforme est issue d'une proposition de loi déposée en 1998 par le député Geert Bourgeois (59). L'intention était de permettre l'utilisation de la télécopie (fax) dans la procédure judiciaire, même si le courrier électronique était déjà timidement mentionné. La législature arriva à son terme sans que cette proposition ait pu être adoptée. Une nouvelle proposition fut introduite par le même auteur lors de la législature suivante (60). Plus ambitieux, le texte en projet prévoyait cette fois une utilisation plus systématique du courrier électronique. Les travaux parlementaires indiquaient toutefois que la notification par pli judiciaire électronique n'était pas visée (61).

Entre-temps complétée par des dispositions de droit civil concernant la signature électronique, cette proposition est à l'origine de la loi du 20 octobre 2000 (62). Les dispositions de cette loi modifiant le Code judiciaire devaient entrer en vigueur à une date déterminée par le

---

(57) Comme nous y invite d'ailleurs l'article 8, § 7, de la loi du 5 août 2006 modifiant certaines dispositions du Code judiciaire en vue de la procédure par voie électronique.

(58) Comme en général d'ailleurs. Cf. notre étude, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcée », in *Commerce électronique : de la théorie à la pratique*, Cahiers du CRID, n° 23, Bruxelles, Bruylant, 2003, p. 69 et s.

(59) *Doc. parl.*, Ch. repr., n° 1501/1, sess. ord. 1997-1998.

(60) *Doc. parl.*, Ch. repr., n° 38/1, sess. extr. 1999.

(61) Rapport de la Commission de la justice, *Doc. parl.* 38/8, session ord. 1999/2000 , p. 41.

(62) Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, p. 42.698.

Roi (63). En réalité, elles ne sont jamais entrées en vigueur, notamment en raison du sous-équipement des cours et tribunaux en moyens informatiques.

29. Il est inutile de s'attarder longuement sur la teneur d'une réforme légale qui n'a pas vu le jour. D'autant qu'avec le recul, elle apparaît timide et maladroite. En effet, elle n'envisageait que l'envoi simple et recommandé, à l'exclusion du pli judiciaire, et repose sur une analyse nettement insuffisante des procédés envisagés.

Ainsi, l'article 4 de la loi du 20 octobre 2000 prévoit-il de compléter l'article 32 du Code judiciaire par un alinéa libellé comme suit : « *Une communication, une notification ou un dépôt qui doivent avoir lieu par lettre recommandée à La Poste, peuvent également avoir lieu valablement par télécopie ou par courrier électronique, pour autant que le destinataire fournisse un accusé de réception* ».

Se faisant l'écho des critiques que nous avions formulées (64), le législateur de 2006 reconnaît que cette disposition était « inadéquate parce qu'imprécise et source d'insécurité juridique » (65).

30. L'intervention d'un tiers neutre – La Poste –, qui s'interpose entre l'émetteur et le destinataire, n'est pas de mise ici, alors qu'il s'agit d'un aspect essentiel du service de recommandé traditionnel. C'est ce tiers qui atteste la réalité et la date de l'envoi. En cas de recours au recommandé avec accusé de réception, La Poste atteste en outre la remise du pli au destinataire ou encore son refus de le recevoir. Dans la loi de 2000, ce schéma tripartite est remplacé par une communication directe entre parties, avec tous les aléas que cette solution entraîne sur le plan probatoire. D'abord, l'émetteur n'est pas à l'abri de la mauvaise foi du destinataire, qui peut s'abstenir d'accuser réception du message reçu, obligeant ainsi l'auteur à effectuer un nouvel envoi par lettre recommandée. Le retard qui en résulte peut avoir des conséquences néfastes si le pli devait être envoyé dans un délai strict. Ensuite, l'accusé de réception n'apporte pas la preuve de la date d'envoi dans la mesure où, pour diverses raisons (négligence, absence...), le destinataire peut tarder à renvoyer l'accusé de réception. Enfin, des contestations peuvent surgir concernant la réalité de l'envoi de l'accusé de réception ou l'identité de son auteur. En effet, à défaut de signature, rien n'empêche le destinataire qui a effectivement expédié

---

(63) Article 7, alinéa 1er, de la loi.

(64) E. Montero, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcée », *op. cit.*, p. 97.

(65) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 30.

un accusé de réception de contester après coup avoir envoyé un tel accusé (66).

En réalité, la disposition commentée ne consacrait nullement dans l'environnement électronique un équivalent fonctionnel du service de recommandé postal, mais conférait à un mécanisme nouveau des effets juridiques comparables à ceux de l'envoi recommandé (67). Cette innovation était inopportune puisque, après avoir évacué l'intervention d'un tiers, elle aurait impliqué le recours à un prestataire de confiance pour procurer un minimum de sécurité probatoire.

B. – Acte II : une réforme plus ambitieuse et plus heureuse

31. Le législateur de 2006 a nettement revu sa copie. Il corrige les imperfections du passé, tout en réalisant une réforme plus ambitieuse. *Primo*, les dispositions de droit judiciaire de la loi du 20 octobre 2000 sont abrogées (68). *Secundo*, la question des envois recommandés est abordée autrement. *Tertio*, la disposition régissant le pli judiciaire est revisitée, notamment pour faire droit au pli judiciaire électronique.

Notre propos se concentre sur le pli judiciaire et le recommandé (entièrement) électroniques. Les autres aspects de la réforme sont à peine évoqués, le lecteur étant renvoyé pour le surplus à la contribution de D. Mougenot.

32. Actuellement, les modalités d'envoi du pli judiciaire sont précisées de façon très détaillée par l'article 46 du Code judiciaire. Cette disposition a été largement remaniée par l'article 8 de la loi du 5 août 2006. En sa nouvelle mouture, l'article 46 compte désormais sept paragraphes.

Les deux premiers réglementent le pli judiciaire traditionnel, notifié à la demande soit du ministère public (§ 1er), soit du greffier (§ 2). Dans les deux cas, le courrier est remis par les services de la poste au destinataire. Celui-ci est invité à signé un accusé de réception qui est renvoyé à l'expéditeur ; le refus de signer est relaté par le préposé de la poste.

---

(66) Pour d'autres commentaires en ce sens, V. LAMBERTS, « Les relations Barreau-Palais : le rôle électronique et la diffusion des données jurisprudentielles » in J.-F. HENROTTE et Y. POULLET (dir.), *Cabinets d'avocats et technologies de l'information – Balises et enjeux*, Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, spéc. pp. 279 et s.

(67) Apparemment en ce sens, M. E. STORME, « Het verrichten van rechtshandelingen door middel van nieuwe telecommunicatiemiddelen – De nieuwe wetsbepalingen ingekaderd in de algemene leer van de kennisgeving », n° 24, http://www.storme.be/2281.pdf.

(68) Article 28 de la loi du 10 juillet 2006 qui abroge les articles 4 à 7 de la loi du 20 octobre 2000. Pour rappel, ces dispositions ne sont jamais entrées en vigueur.

Jusqu'ici, aucune modification n'est apportée au texte en vigueur, si ce n'est le remplacement de la référence à La Poste par les termes « services postaux » (69).

Le nouveau paragraphe 3 de l'article 46 consacre une forme hybride du pli judiciaire. L'idée est simple : le pli est envoyé par le greffier ou le ministère public à un prestataire de services de communication, qui est chargé de l'imprimer et de le faire parvenir à son destinataire. Le texte prend soin de préciser que le PSC *« peut attester que le pli adressé au destinataire est conforme à celui envoyé par le greffier ou le ministère public ; il peut également attester la date à laquelle il a remis le pli aux services postaux ou l'a fait parvenir au destinataire »*. La technique du pli judiciaire ou recommandé hybride est commentée dans d'autres contributions. Contentons-nous de remarquer qu'elle a fait l'objet de vives réserves de la part de certains auteurs. Toutefois, leurs objections concernent plus particulièrement le service de recommandé hybride offert par Certipost et, singulièrement, les difficultés que ce procédé suscite dans les communications entre avocats et entre ces derniers et leurs clients (70). Leurs critiques perdent une partie de leur poids s'agissant du nouveau texte relatif au pli judiciaire dans la mesure où le PSC n'est pas n'importe quelle entreprise offrant un service de recommandé électronique mais un prestataire soumis à des obligations strictes, notamment en matière de confidentialité (71), et qui est investi du pouvoir d'attester la conformité à l'original du contenu et de la signature du pli.

Le nouveau paragraphe 4 de l'article 46 consacre le pli judiciaire (entièrement) électronique, qui nous intéresse plus particulièrement : *« sans préjudice de l'application des conventions internationales en la matière, le pli judiciaire peut être adressé par voie électronique.*

Il est délivré à l'adresse judiciaire électronique, par l'intermédiaire d'un prestataire de services de communication tel que visé à l'article 2, 4°,

---

(69) Cette modification prend acte de la libéralisation du service des envois recommandés électroniques, le monopole de La Poste ne subsistant que pour les envois recommandés physiques (entendez sur support papier) réalisés dans le cadre de procédures judiciaires ou administratives. Cf. l'article 144*octies* de la loi du 21 mars 1991 sur les entreprises publiques économiques, modifié par l'article 172 de la loi-programme du 2 août 2002.

(70) Cf. D. Fesler, « La correspondance et le recommandé électroniques dans les relations entre avocats », in J.-F. Henrotte et Y. Poullet (dir.), *Cabinets d'avocats et technologies de l'information – Balises et enjeux*, Cahiers du CRID, n° 26, Bruxelles, Bruylant, 2005, p. 237 ; J.-F. Henrotte, « L'encadrement des transactions électroniques réalisées via le réseau et les questions de responsabilité professionnelle », dans le même ouvrage, pp. 89-90 ; J.-F. Henrotte et D. Fesler, « Phenix : du mythe à la pratique. Questions sur la procédure électronique en matière civile et pénale », in J.-F. Henrotte (coord.), *Phenix et la procédure électronique*, CUP, vol. 85, Bruxelles, Larcier, 2/2006, p. 223.

(71) Sur le projet d'arrêté royal, voy. *infra*, n° 52.

de la loi du 10 juillet 2006 relative à la procédure par voie électronique (…) ».

Les deux paragraphes suivants sont relatifs aux formes et mentions du pli judiciaire (§ 5) et au remplacement des notifications par des significations dans certaines circonstances (§ 6). La substance des dispositions de l'ancien texte reste inchangée (les paragraphes 3 et 4). On relève néanmoins que la détermination des formes et mentions ressortit désormais à la compétence du Ministre de la justice et non plus à celle du Ministre qui a l'administration des postes dans ses attributions. Sur le plan de la rédaction, les dispositions subissent de légères retouches : d'une part, certains termes imprégnés de la culture du papier (enveloppe…) ont disparu, d'autre part, les termes « la poste » ont été remplacés par « les services postaux ».

Enfin, le dernier paragraphe de l'article 46 précise que *« les modalités d'envoi par pli judiciaire s'appliquent à l'envoi recommandé avec accusé de réception ».*

Même si le Code judiciaire prévoit, en divers cas, la notification par pli recommandé avec accusé de réception, il ne souffle mot sur les modalités de ce mode de communication. Le paragraphe 7 déclare applicables au recommandé avec accusé de réception les règles relatives au pli judiciaire. Les deux mécanismes étant similaires, sous réserve de petites différences formelles, il convenait que leurs modalités d'envoi soient identiques. Le nouveau paragraphe le précise clairement, sous une forme qui évite de fastidieuses répétitions.

33. On ajoutera, enfin, que le Code judiciaire permet aussi des dépôts ou communications par pli recommandé (simple). À ce propos, la loi du 5 août 2006 précise, en son article 4, ce qui suit : *« Tout dépôt ou communication peut avoir lieu valablement par pli simple ou, dans les cas prévus par la loi, par pli recommandé.*

Les dépôts ou communications par pli simple ou recommandé adressés au greffe et au parquet peuvent avoir lieu valablement par voie électronique par introduction dans le système Phenix.

Toute autre communication par pli simple peut avoir lieu valablement par courrier électronique à l'adresse judiciaire électronique.

Toute autre communication par lettre recommandée peut avoir lieu valablement par courrier électronique à l'adresse judiciaire électronique, pour autant qu'une preuve d'envoi soit remise à l'expéditeur. Cette preuve d'envoi ne peut être créée automatiquement par le système d'expédition de l'expéditeur. » (art. 32*bis* nouveau, C. jud.).

34. L'état des lieux dressé, il convient à présent de livrer une première analyse critique des textes. Notre propos est plus

précisément d'apprécier si les mécanismes du pli judiciaire et de l'envoi recommandé ont été adéquatement transposés dans l'environnement électronique. Le moment de la prise d'effet des actes de procédure par pli judiciaire ou pli recommandé ne sera pas envisagé, cette délicate question étant traitée dans la contribution de D. Mougenot.

Notre méthode d'analyse consistera à soumettre les nouveaux dispositifs institués au test de l'équivalence fonctionnelle : il s'agit, en d'autres termes, de les jauger au regard des fonctions traditionnellement dévolues aux plis judiciaire et recommandé.

§ 2. Le test de l'équivalence fonctionnelle

A. – Les fonctions assignées au recommandé

35. Pour la clarté de l'exposé, on commence par rappeler brièvement les fonctions traditionnellement dévolues au service d'envoi recommandé (72).

L'envoi recommandé est un « service consistant à garantir forfaitairement contre les risques de perte, vol ou détérioration, et fournissant à l'expéditeur, le cas échéant à sa demande, une preuve du dépôt ou de l'envoi postal et/ou de sa remise au destinataire » (73).

Il ressort de cette définition que la garantie contre les risques de perte, vol ou détérioration est l'une des fonctions centrales du recommandé (74). On pourrait même penser que « la preuve de l'envoi et de la réception ne sont, d'un point de vue strictement légal, que des éléments adventices et facultatifs de la définition du recommandé » (75). On n'est cependant pas obligé d'adhérer à ce point de vue : nonobstant sa rédaction ambiguë, cette disposition fait de la remise d'une preuve du dépôt ou de l'envoi postal une fonction essentielle du recommandé. L'expression « le cas échéant à sa demande » vise la seule preuve de la remise au destinataire.

---

(72) Pour un développement plus détaillé et nuancé, E. Montero, « Du recommandé traditionnel au recommandé électronique : vers une sécurité et une force probante renforcées », in *Commerce électronique : de la théorie à la pratique*, Cahiers du CRID, n° 23, Bruxelles, Bruylant, 2003, pp. 69-99.

(73) Article 131, 8°, de la loi du 21 mars 1991 portant réforme de certaines entreprises économiques.

(74) Pour plus de détails sur l'étendue de la responsabilité de La Poste, l'indemnité due en cas de perte, de spoliation ou d'avarie d'un envoi recommandé et le montant maximum de la déclaration de valeur d'une lettre avec valeur déclarée, voy. notre étude précitée « Du recommandé traditionnel au recommandé électronique… », note 23.

(75) En ce sens, D. Fesler, « La correspondance et le recommandé électronique dans les relations entre avocats », *op. cit.*, p. 235.

36. *La preuve de l'envoi.* – L'intérêt incontestable de toute lettre recommandée est de ménager à l'expéditeur une preuve de la réalité et, au besoin, du moment de son envoi, *ou plus exactement de son dépôt à La Poste*. Cette double preuve pourra être rapportée grâce au récépissé qui lui est remis par l'agent de La Poste lors du dépôt du pli.

37. *La preuve de la réception.* – Par contre, le dépôt à La Poste d'une lettre recommandée n'atteste nullement que celle-ci est effectivement parvenue à son destinataire. L'occasion a été donnée à la jurisprudence de confirmer ce point de vue (76). L'éventualité qu'un envoi recommandé s'égare et n'arrive jamais à destination est d'ailleurs clairement envisagée dans les dispositions fixant la hauteur de l'indemnité due par La Poste en cas de perte, de vol ou de détérioration d'un envoi recommandé. En tout état de cause, le destinataire peut toujours prétendre n'avoir pas reçu le courrier recommandé que l'expéditeur affirme avoir déposé à La Poste.

L'expéditeur peut toutefois se prémunir contre ce risque, en faisant recours à un type particulier de recommandé : le *recommandé avec accusé de réception*. Dans cette hypothèse, le destinataire est invité à signer un accusé de réception du courrier qui lui est présenté par le facteur. Ce dernier doit vérifier l'identité du destinataire et remettre la lettre en mains propres. En principe, l'expéditeur sera alors en mesure de prouver que la réception de son envoi a bien eu lieu à la date et à l'heure indiquées sur l'accusé.

38. *La preuve du contenu de l'envoi.* – Encore des contestations peuvent-elles surgir à propos du contenu de l'envoi recommandé. À cet égard, La Poste ne procède à aucune vérification. Dès lors, tout en ne contestant pas avoir reçu le courrier recommandé (77), le destinataire peut prétendre que l'enveloppe était vide ou que la copie de la lettre qui s'y trouvait ne correspond pas à l'original conservé et produit ultérieurement par l'expéditeur. Ces problèmes sont assurément délicats, même s'il faut souligner leur extrême rareté.

Le recours à l'envoi recommandé (éventuellement avec accusé de réception) permet de présumer, jusqu'à preuve contraire, que le desti-

---

(76) Par exemple, Mons, 21 octobre 1998, *J.L.M.B.*, 1999, I, p. 456 : « Le seul fait pour les services de La Poste d'apposer pour chaque envoi individuel un cachet établissant l'envoi recommandé n'apparaît pas suffisant pour en déduire que le destinataire a reçu l'envoi qui lui était destiné ou qu'il en a eu connaissance (...) ».

(77) Cette contestation serait vaine en cas d'envoi recommandé avec accusé de réception. Le juge disposera, en effet, de deux pièces (le récépissé et l'accusé de réception) qui attestent que la lettre est effectivement parvenue à son destinataire (sauf si l'accusé de réception est signé par un autre, auquel cas c'est la responsabilité de La Poste qui pourra éventuellement être engagée).

nataire a reçu le courrier invoqué par l'émetteur (78). Si le destinataire conteste le contenu de l'enveloppe, en soutenant qu'elle était vide, il lui faudra fournir la preuve de cette allégation contraire au *cours normal et habituel des choses* (79). Vu que la contestation porte sur un fait juridique, cette preuve peut être administrée par toutes voies de droit. La démonstration de la sincérité, ou au moins de la vraisemblance, de l'affirmation selon laquelle l'enveloppe reçue était vide pourrait résulter aux yeux du juge des démarches et investigations effectuées par le destinataire, immédiatement après la réception de l'envoi, auprès de La Poste ou de l'expéditeur, afin d'identifier l'auteur de cette curieuse correspondance et de s'enquérir de ses intentions (80).

Le même genre de solution prévaut en cas de contestation portant sur le contenu de l'enveloppe ou du document lui-même. Ainsi, il a été jugé que la preuve que deux lettres se trouvaient dans une enveloppe recommandée exige que l'invraisemblance du fait soit renversée par des éléments précis (81).

39. *Récapitulatif.* – Au total, le recommandé postal est une institution relativement modeste eu égard aux garanties qu'elle apporte. Outre la garantie contre les risques de perte, vol ou détérioration, le dépôt à La Poste d'une lettre recommandée permet tout au plus d'établir la date du dépôt (sans certitude que la lettre soit parvenue à destination !) et, le cas échéant, sa bonne réception par le destinataire (recommandé avec accusé de réception). Pour le reste, il faut s'en remettre à de simples présomptions – fussent-elles sérieuses –, qui trouvent

---

(78) Ayant eu à se prononcer à ce sujet, la Cour de cassation française a estimé que « *la remise d'une [lettre recommandée avec accusé de réception] fait présumer, jusqu'à preuve contraire, que la notification [d'un congé, en l'espèce] était régulière* », et qu'il appartient dès lors au destinataire qui affirme avoir reçu une enveloppe vide d'apporter des éléments de preuve à l'appui de son allégation. Cf. Cass. fr. (ch. civ., sect. soc.), 11 juin 1964, *J.T.*, 1965, p. 120. Dans le même sens : Civ. Verviers, 13 mai 1925, *Jur. Liège*, 1925, p. 220.

(79) Cf. H. De Page, *Traité*, t. III, 3e éd., 1967, p. 731, n° 726. Voir aussi N. Verheyden-Jeanmart, *Droit de la preuve*, Bruxelles, Larcier, 1991, p. 40, n° 65 ; M. Antoine, « La certification électronique », *R.D.C.*, 1995, p. 6 ; D. Mougenot, *La preuve*, *op. cit.*, p. 244, n° 180.

(80) Voy., p.ex., Civ. Verviers, 13 mai 1925, *J.L.*, 1925, p. 221 : « Que, d'ailleurs, si par impossible et quelque invraisemblable que cela puisse paraître en la cause, l'appelant avait par inadvertance omis d'insérer dans l'enveloppe le congé, encore est-il que l'intimé (...) serait en faute pour n'avoir fait aucune démarche ou investigation en vue de démontrer que l'enveloppe reçue par lui ne contenait aucun écrit ».

(81) Comm. Bruxelles, 30 juin 1982, *Rev. prat. soc.*, 1984, p. 59. En l'espèce, une partie alléguait que la lettre notifiant une cession d'actions au porteur figurait dans le même pli recommandé qu'une autre lettre relative à la convocation d'une assemblée générale. Cette allégation, contestée par la partie adverse, apparaît invraisemblable aux yeux du juge, en considération d'indices divers : « qu'en effet, seule la lettre relative à la demande de convocation d'une assemblée générale porte la mention 'recommandé' ; que si l'autre lettre avait été jointe au même envoi, elle eût normalement porté la même mention ; que l'on remarque aussi que les caractères d'imprimerie utilisés pour ces lettres ne sont pas les mêmes, alors qu'elles sont signées par la même personne ; (...) ».

leur justification dans le fonctionnement globalement satisfaisant des services postaux (les lettres parviennent d'ordinaire à leur destinataire) et dans une présomption, jusqu'à preuve contraire, en faveur de la situation normale et habituelle (contenu de l'envoi). Il convient de se le rappeler au moment d'évaluer les formes électroniques de l'institution admises dans le cadre des communications judiciaires.

B. – Les formes électroniques du recommandé dans la procédure judiciaire

40. La loi du 5 août 2006 institue trois formes d'envoi d'un recommandé électronique. On les examine tour à tour.

1. *Les dépôts ou communications par pli recommandé*

41. L'on sait que les justiciables ou leurs avocats, les huissiers, experts... sont amenés à adresser des actes de procédure (dépôt) ou d'autres informations quelconques, dont l'envoi ne fait pas l'objet d'une réglementation spécifique (communication), au greffe ou au parquet par pli simple ou, dans certains cas prévus par la loi, par pli recommandé.

a) L'article 32*bis*, alinéa 2 (nouveau) du Code judiciaire

42. Dorénavant, ces dépôts ou communications par pli (simple ou) recommandé peuvent *« avoir lieu valablement par voie électronique par introduction dans le système Phenix »* (82). Pratiquement, les intéressés se rendent sur le site web de Phenix où ils sont invités à compléter en ligne un formulaire et à y attacher l'acte de procédure concerné. Le système horodate automatiquement le moment où l'acte est introduit et un accusé de réception est délivré. On remarquera qu'on s'éloigne du schéma tripartite caractéristique du service de recommandé traditionnel. Il n'y a pas ici d'intervention d'un prestataire de services de communication, ni d'aucun autre tiers, dans la communication. Celle-ci s'établit directement entre l'utilisateur et le système Phenix. Est-ce un problème ?

Force est de constater qu'en ce qui concerne les actes accomplis au greffe par introduction directe dans le système Phenix, l'intéressé dispose immédiatement d'une preuve de la réalité et de la date de son envoi (horodatage du moment où l'acte a été envoyé/reçu et expédition automatique d'un récépissé attestant cette date), ce qui n'était pas le cas avec la solution adoptée par la loi du 20 octobre 2000. Même si aucun tiers neutre n'intervient dans la communication, nous avons bien

(82) Loi du 5 août 2006, article 4, insérant un article 32*bis* dans le Code judiciaire.

affaire ici à un équivalent fonctionnel du recommandé traditionnel, la fonction essentielle de ce type d'envoi étant assurée (83). Mieux : l'expéditeur est certain que son pli est parvenu à destination (84), ce qui n'est pas le cas avec le recommandé postal, et l'intégrité du contenu est préservée (dès lors qu'il s'agit là d'une des fonctions assurées par la signature qualifiée dont doivent être porteurs la plupart des actes adressés au greffe).

b) L'article 32*bis*, alinéa 4 (nouveau) du Code judiciaire

43. Les autres communications par lettre recommandée, à savoir toutes celles qui ne s'adressent pas au greffe ou au parquet, peuvent « *avoir lieu valablement par courrier électronique à* ***l'adresse judiciaire électronique****, pour autant qu'une preuve d'envoi soit remise à l'expéditeur. Cette preuve d'envoi ne peut être créée automatiquement par le système d'expédition de l'expéditeur* ».

Comme rappelé plus haut (*supra*, n° 28), la loi du 20 octobre 2000 avait déjà prévu le recours au courrier électronique pour réaliser une communication, une notification ou un dépôt qui doivent avoir lieu par lettre recommandée pourvu, d'une part, que le destinataire indique une adresse électronique ou l'utilise régulièrement, d'autre part, qu'il fournisse un accusé de réception (art. 4, modifiant l'art. 32 C. jud.).

Cette disposition était source d'insécurité juridique. En effet, le texte n'indiquait pas dans quel contexte et sous quelle forme le destinataire doit indiquer son adresse électronique : *quid* si une personne utilise plusieurs adresses de courrier électronique ? *quid* en cas de changement d'adresse ? qu'est-ce qu'une utilisation régulière ? Par ailleurs, l'envoi de l'accusé de réception était soumis au bon vouloir du destinataire : on a déjà souligné les aléas que cette solution comportait (*supra*, n° 30).

44. Aussi le nouveau texte prévoit-il que le courrier électronique peut être expédié à l'adresse judiciaire électronique (85). On évite ainsi les hésitations relatives à la détermination de l'adresse électronique utilisée pour des communications judiciaires.

Par ailleurs, il n'est plus indiqué que le destinataire doit fournir un accusé de réception. La seule condition d'assimilation de la communication par courrier électronique au recommandé est qu'une preuve

(83) Sous réserve de l'absence de garantie contre la perte, la détérioration ou l'appropriation par un tiers. Ces risques peuvent néanmoins être efficacement conjurés à la faveur de rigoureuses mesures de sécurité adoptées au niveau du système Phenix.

(84) Il est également averti en cas de refus (p.ex. en raison d'un virus affectant le document).

(85) Sur ce concept, voy. la contribution de I. VEROUGSTRATE.

d'envoi soit remise à l'expéditeur, sans qu'elle puisse toutefois être créée automatiquement par le système d'expédition de ce dernier (86). Notons que cette formulation n'exclut pas formellement que l'accusé de réception puisse émaner du destinataire. Néanmoins, cette solution n'offrant pas de garantie à l'expéditeur, elle ne paraît pas envisageable.

45. Les travaux parlementaires suggèrent que la preuve d'envoi peut être créée par une entreprise offrant un service de recommandé électronique, comme il en existe plusieurs sur le marché. Toutefois, précisent-ils encore, « le texte reste volontairement assez général, pour ne pas fermer la porte à d'autres formes de **recommandé électronique** qui pourraient apparaître ultérieurement sur le marché » (87). Ces considérations sous-entendent que tout mécanisme électronique peut convenir à condition que la fonction essentielle du recommandé – attester la réalité et la date de l'envoi – soit préservée. Si telle est l'intention du législateur, pourquoi n'impose-t-il pas clairement le recours au recommandé électronique, ce qui est possible sans préjuger de la forme de ce dernier ? Par exemple, il aurait pu s'exprimer comme suit : « Toute autre communication par lettre recommandée peut avoir lieu valablement par recommandé électronique à l'adresse judiciaire électronique ».

En réalité, cette rédaction aurait contraint le législateur à définir la notion de « recommandé électronique », sinon son régime juridique, ce qu'il voulait précisément éviter, entendant se borner à édicter les règles applicables à la communication judiciaire (88). Cette réserve est louable et de bonne méthode : le recommandé électronique ayant vocation à s'appliquer bien au-delà du domaine de la procédure judiciaire, il eut été regrettable d'en dessiner les contours juridiques dans ce cadre particulier.

Le libellé de l'article 32*bis*, alinéa 4 (nouveau), du Code judiciaire paraît astucieux. Centré sur l'exigence essentielle du recommandé, il semble requérir, dans la communication électronique, le recours à un équivalent fonctionnel de l'envoi recommandé traditionnel. Tout se passe comme si le législateur avait réussi à imposer le recours au recommandé électronique, tout en évitant de devoir définir la notion.

---

(86) En effet, il n'est pas difficile de produire une copie imprimée d'un courrier électronique portant les mentions de date créées par l'ordinateur. Pareils éléments ne sont dès lors pas probants pour être admis à titre de preuve d'un envoi équivalent au recommandé en matière judiciaire.

(87) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 31. Souligné par nous.

(88) Cf. *ibid.*, en note.

Néanmoins, *primo*, la garantie contre les risques de perte, vol ou détérioration a été perdue de vue ; aucune indication n'est fournie en ce qui concerne le montant de l'indemnité due dans ces circonstances. Mais, enfin, l'intérêt de payer un montant forfaitaire à l'expéditeur d'un pli qui s'est perdu est bien mince lorsque celui-ci devait servir à introduire une procédure et interrompre la prescription. Le préjudice est sans commune mesure avec l'indemnité réglementaire. *Secundo*, et ce point est plus gênant, le texte n'empêche pas le recours à l'un de ces services de courrier électronique offerts sur le marché qui, tout en procurant une preuve d'envoi, n'offrent aucune garantie (solidité financière, continuité des activités, mesures de sécurité, fiabilité des technologies utilisées, confidentialité...).

À la réflexion, pour assurer une équivalence parfaite entre le recommandé postal et son homologue électronique, une référence directe au recommandé électronique eut été préférable. On ne saurait cependant blâmer le législateur de 2006 qui s'est heurté à l'absence de loi-cadre fixant un statut juridique pour les prestataires de confiance (89).

2. *La notification par pli judiciaire (entièrement) électronique*

46. Le pli judiciaire, qui – rappelons-le – s'apparente à l'envoi recommandé avec accusé de réception, peut être adressé par voie électronique. En ce cas, il est délivré à l'adresse judiciaire électronique par l'intermédiaire d'un prestataire de services de communication (90).

Ce mécanisme se caractérise par deux traits saillants : l'envoi doit nécessairement transiter par le PSC et doit être adressé à l'adresse judiciaire électronique. Pourquoi l'intervention obligatoire d'un PSC ? Pour garantir la bonne fin de l'opération sur le plan technique, ce que le greffier ou le secrétaire de parquet ne peut faire, à défaut de disposer des connaissances et du matériel adéquats. Le pli est envoyé exclusivement à l'adresse judiciaire électronique, qui est la seule que le destinataire a explicitement choisie pour ce type de communications. Dans un premier temps, l'utilisation de cette forme de pli judiciaire sera assez limitée, sauf si la formule de l'adresse judiciaire électronique connaît un succès rapide ou si le Roi en impose l'usage à certaines catégories de justiciables (les autorités publiques par exemple).

Que se passe-t-il si la communication électronique vers le destinataire échoue ? Dans cette hypothèse, l'envoi doit être recommencé par

---

(89) Comme on le verra, un avant-projet de loi sur certains prestataires de confiance définit, entre autres services, le recommandé électronique en des termes plus conformes au principe d'équivalence ; surtout, il fixe les obligations et responsabilités des prestataires de pareils services (*infra*, n° 52).

(90) Article 46, § 4 (nouveau), du Code judiciaire (cf. l'art. 8, § 4, de la loi du 5 août 2006).

voie postale traditionnelle ou par voie hybride. La loi dispose en effet que : *« si dans les vingt-quatre heures de l'envoi par le greffe ou le ministère public, le prestataire de services de communication ne fait pas parvenir au greffe ou au ministère public un avis de délivrance de celui-ci, la notification a lieu sans délai, selon les cas conformément aux §§ 1er, 2 ou 3 ».*

47. Comme nous le verrons ci-après, toutes les fonctions du pli judiciaire/du recommandé avec accusé de réception sont ici préservées (91). Ainsi, le PSC est tenu des obligations suivantes : vérifier l'identité des parties, assurer que les dates et heures d'envoi et de délivrance (92) des actes de procédure puissent être déterminées avec précision, communiquer sans délai à l'expéditeur ces données et enregistrer toutes les informations pertinentes relatives aux communications effectuées pendant trente ans, en particulier pour pouvoir fournir une preuve de la certification en justice (93).

Section 3. – Le statut du prestataire de services de communication

48. Le prestataire de services de communication (PSC) joue un rôle central dans le système Phenix. Cet intervenant appartient à la famille des tiers de confiance. Les travaux parlementaires précisent que l'expression « prestataire de services de communication » a été choisie par parallélisme avec la terminologie utilisée dans la loi du 9 juillet 2001 qui traite des « prestataires de service de certification » (94).

Par les fonctions qu'il est appelé à remplir, le PSC s'apparente largement à un prestataire de service de recommandé électronique. Logiquement, son statut juridique ne devrait pas être fondamentalement différent de celui des prestataires de tels services, quitte à prévoir certaines obligations additionnelles vu qu'il est appelé à œuvrer dans le secteur sensible de la communication judiciaire. En tout cas, on comprendrait mal que ses obligations et responsabilités soient moins rigoureuses que celles des prestataires de service de recommandé électronique.

---

(91) Sous réserve de la garantie contre les risques de perte, détérioration ou appropriation par des tiers ?

(92) Aux termes de l'article 9, § 3, de la loi du 10 juillet 2006 : « la délivrance d'un document électronique est le moment où le destinataire peut prendre connaissance du contenu de celui-ci ».

(93) Article 10, § 1er, 1°, 2°, 5° et 7°.

(94) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 13.

Une loi fixant un cadre juridique pour certains prestataires de services de confiance (notamment les prestataires de service de recommandé électronique) est actuellement en préparation. Grâce à un vent favorable, ce texte est en notre possession (95). Evidemment, l'idéal aurait été que ce texte soit adopté et entre en vigueur avant les textes régissant le système Phenix. Ceux-ci se seraient alors contenté de renvois opportuns et l'on aurait évité tout risque d'incohérence. Les auteurs des textes régissant la procédure électronique en conviennent (96). Malheureusement, le calendrier arrêté pour la mise en œuvre du projet Phenix n'a pas permis d'attendre l'adoption de cette loi régissant le statut juridique des différents tiers de confiance. Aussi a-t-il été décidé de prévoir, dans la loi du 10 juillet 2006, les grandes lignes du statut juridique du PSC. Tel est la visée de l'article 10 de la loi. Par ailleurs, un arrêté royal, en préparation, détermine les conditions d'application des exigences fixées par cette disposition.

Notre propos est d'examiner si la coordination entre ces dispositions et celles qui seront applicables, demain, aux prestataires de service de recommandé électronique est satisfaisante. Étant donné que l'arrêté royal en question et la loi en projet sur certains prestataires de services de confiance risquent de subir des modifications au cours de leur gestation politique, des références précises à leurs dispositions semblent inutiles. On se contentera d'émettre quelques réflexions générales.

§ 1. Bref commentaire de l'article 10 de la loi du 10 juillet 2006

49. Les dispositions de l'article 10 sont inspirées de l'annexe II de la loi du 9 juillet 2001, qui précise les exigences concernant les prestataires de service de certification délivrant des certificats qualifiés. Toutefois, les exigences propres à la certification de signature n'ont logiquement pas été reprises ; à l'inverse, le rôle d'intermédiaire dans la communication judiciaire présente certaines spécificités dont il fallait tenir compte.

50. Aux termes de l'article 10, § 1er, le PSC doit répondre aux exigences suivantes :

1° assurer que puissent être déterminées avec précision la date et l'heure des communications. Cette prestation est centrale parmi les tâches dévolue au PSC.

---

(95) En réalité, une légère brise a suffi puisque nous avons eu le privilège de diriger la rédaction de cet avant-projet de loi dans le cadre d'une convention de recherche pour le compte du Ministre de l'Économie. Une partie de ce texte a été détachée et d'ores et déjà soumise au Gouvernement qui l'a approuvée en seconde lecture au mois d'octobre dernier.

(96) Projet de loi relatif à la procédure par voie électronique, Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1701/001 du 11 avril 2005, p. 24.

2° vérifier, par des moyens appropriés et légaux, l'identité des parties à la communication. Certaines formes de communication judiciaire, telles la signification ou la notification par pli judiciaire, supposent en tout cas la vérification de l'identité du destinataire. Par ailleurs, lorsque la communication émane d'un parquet, d'un tribunal ou d'un greffe, le tiers doit pouvoir en vérifier l'origine. Il importe donc que le PSC maîtrise ces techniques, tout en veillant au respect des règles légales, notamment celles relatives à la protection de la vie privée.

3° utiliser des systèmes et des produits fiables. Le PSC est tenu de recourir à des procédés techniquement sûrs et éprouvés, qui garantissent l'intégrité et, plus généralement, la sécurité des communications.

4° garantir la confidentialité des données dont il assure la transmission ou la conservation. S'agissant de données relatives à des actes de procédure, cette garantie est naturellement fondamentale.

5° enregistrer toutes les informations pertinentes relatives aux communications pendant un délai de trente ans. Cette période tient compte des longs délais de recevabilité d'une tierce opposition.

6° respecter les délais imposés par l'expéditeur afin de permettre à celui-ci de se conformer aux délais légaux. Cette exigence tient au fait que les délais à respecter pour procéder à une signification, une notification, un dépôt ou une communication sont parfois très courts. En cas de retard dans l'envoi occasionnant un préjudice aux intérêts de l'expéditeur, le PSC engage sa responsabilité. Il appartient néanmoins à l'expéditeur d'indiquer au PSC si un délai particulier doit être respecté. À défaut, il n'est soumis qu'à l'obligation normale de diligence.

7° communiquer sans délai à l'expéditeur les données visées aux points 1° et 2°. Il importe en effet que l'expéditeur sache rapidement si la communication a pu s'effectuer normalement et à quel moment. Il doit pouvoir prendre attitude en cas d'échec de celle-ci.

8° disposer des capacités économiques et financières suffisantes pour assumer l'ensemble de ses obligations, en particulier pour endosser la responsabilité en cas de dommages.

51. L'article 10, § 2, prévoit que nul PSC ne peut être soumis à une autorisation préalable pour exercer ses activités. Cette disposition découle de l'article 4 de la directive sur le commerce électronique (97),

(97) Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce

tout PSC devant être considéré comme un prestataire de service de la société de l'information (98).

Néanmoins, le PSC doit communiquer à l'administration une série d'informations : un rapport justifiant qu'il répond aux exigences fixées à l'article 10, § 1er ; son nom ; son adresse géographique d'établissement ; ses coordonnées ; le cas échéant, son titre professionnel et son numéro d'entreprise. Pour sa part, l'administration est tenue de lui délivrer un récépissé dans les dix jours de cette communication.

Enfin, l'article 10, § 3, prévoit que le PSC peut demander une accréditation volontaire à l'administration, tout en déléguant au Roi le soin de fixer les conditions et modalités de cette procédure.

§ 2. Aperçu des dispositions complémentaires

52. L'arrêté royal (en préparation) portant exécution de l'article 10, § 1er, apporte des précisions supplémentaires sur lesquelles il est inutile de s'étendre à ce stade. Contentons-nous de relever certains points. Ainsi, l'arrêté royal dresse la liste des données que le PSC est tenu d'enregistrer, à savoir l'identité de l'émetteur et du destinataire, divers numéros pertinents (99), l'adresse judiciaire électronique du destinataire, le statut de l'envoi (réceptionné par le PSC, délivré ou non au destinataire), la date et l'heure de ce statut, un rapport pour non-délivrance, les protocoles de communication et de cryptographie, etc. Il fixe certaines exigences relatives à l'accessibilité, l'intégrité et la lisibilité de ces enregistrements. Il détermine les règles applicables aux accusés d'envoi, de réception, de refus ou de non délivrance (données devant y figurer, modalités de communication…). Il précise les obligations du prestataire en cas d'arrêt de ses activités.

Par ailleurs, l'arrêté royal soumet le PSC à une série d'obligations, qui se retrouvent presque à l'identique (sous réserve de formulations différentes) dans le projet de législation sur certains prestataires de confiance. Ainsi doit-il :

électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.C.E.*, n° L 178 du 17 juillet 2000, p. 1.

(98) L'article 4 de cette directive rappelle le principe fondamental de la liberté d'établissement (article 50 du Traité CE). Il a été transposé à l'article 4, alinéa 1er, de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003, p. 12963. Le prestataire y est défini comme « toute personne physique ou morale qui fournit un service de la société de l'information » (article 2, 3°, de la loi). Quant à cette dernière notion, elle s'entend de « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire du service » (art. 2, 1°).

(99) Le numéro de l'affaire concernée par les actes de procédure, le numéro de la pièce dans l'inventaire du service d'expédition, le numéro de suite de l'envoi de la pièce…

- faire preuve d'impartialité vis-à-vis des destinataires de ses services et des tiers ;
- fournir aux destinataires de ses services, avant la conclusion du contrat, un accès facile et direct à une série d'informations formulées de manière claire et distincte : les modalités et conditions précises d'utilisation de ses services ; le fonctionnement et l'accessibilité de ses services ; les mesures qu'il adopte en matière de sécurité ; les procédures de notification d'incidents, de réclamation et de règlement des litiges ; les garanties qu'il apporte ; l'étendue de sa responsabilité ; l'existence ou l'absence d'une couverture d'assurance et, le cas échéant, son étendue (100) ;
- garantir la confidentialité des données transmises tout au long du processus de communication (en sécurisant la ligne de communication entre le système Phenix et l'adresse judiciaire électronique) ;
- employer du personnel ayant les compétences spécifiques nécessaires à la fourniture de ses services ;
- se garder de détourner, à quelque fin que ce soit, les données qui lui sont transmises, lesquelles ne peuvent par ailleurs être consultées que dans la mesure nécessaire à l'accomplissement de ses services ;
- soumettre son personnel à une obligation de confidentialité ;
- disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la loi (relative à la procédure électronique) et ses arrêtés royaux d'exécution, en particulier pour endosser la responsabilité de dommages, en contractant en tout cas (!) une assurance appropriée.

Dans la loi en projet sur certains prestataires de confiance, ces obligations forment un tronc commun d'exigences applicables à tous les prestataires visés par la loi (101). Il est regrettable qu'elles soient reprises, tantôt littéralement, tantôt sous une forme différente quant au fond (parfois) ou à la forme (souvent). Par ailleurs, ce projet de loi contient des prescriptions en matière d'horodatage, d'archivage des données et de numérisation de documents. Or, ces préoccupations ne sont pas absentes du projet Phenix, loin s'en faut. Il fixe également les modalités d'établissement des référentiels techniques relatifs aux services et systèmes concernés. Pour sa part, le projet d'arrêté royal por-

(100) Notons qu'en une autre de ses dispositions, le projet d'arrêté royal impose la souscription d'une assurance (?).

(101) À savoir, les prestataires d'archivage électronique, d'horodatage électronique, de recommandé électronique et de blocage transitoire des sommes versées.

tant exécution de l'article 10, § 1er, ne fait curieusement aucune espèce d'allusion à ce genre de référentiels.

Concernant plus particulièrement le service de recommandé électronique, le projet de loi sur certains prestataires de confiance prend soin de définir la notion : il s'agit d'un *« service de transmission de données électroniques garantissant forfaitairement contre les risques d'appropriation par un tiers, de perte ou de détérioration des données et fournissant par voie électronique au destinataire du service une preuve de leur envoi et, le cas échéant, de leur remise au destinataire des données ».* Cette définition a le mérite d'être rigoureusement respectueuse du principe de l'équivalence fonctionnelle. La loi en projet fixe aussi, par référence, le montant de l'indemnité due en cas de perte, d'appropriation ou d'altération du contenu du message par un tiers, alors que cette précision est absente dans le projet d'arrêté royal.

53. Il n'est pas nécessaire de pousser plus avant la lecture comparée de ces textes. Les indications fournies suffisent pour se faire une idée générale du statut du PSC et attirer l'attention sur l'importance et l'urgence d'une concertation. À défaut, on risque de soumettre des activités similaires, qu'elles soient assumées par des PSC ou d'autres prestataires de services de confiance, à un faisceau de règles aussi disparates qu'incohérentes.

CONCLUSION

54. Sur les questions qui ont retenu notre attention, les textes régissant la procédure judiciaire électronique sont globalement satisfaisants. Le législateur a été bien avisé d'imposer le recours à la signature qualifiée en matière d'actes de procédure. Par ailleurs, les fonctions traditionnelles du recommandé ont été généralement bien restituées dans les dispositions relatives aux plis judiciaire et recommandé électroniques.

En ce qui concerne le statut du prestataire de services de communication, nous avons épinglé le risque de dispersion des règles et d'incohérence eu égard au projet parallèle de législation concernant certains services de confiance. Faut-il que la mise en œuvre du projet Phenix s'enferme dans un calendrier infernal ? Le mieux serait d'anticiper l'adoption de la loi générale sur certains prestataires de confiance et de se limiter, dans le cadre du projet Phenix, aux règles destinées à prendre en compte les seules spécificités inhérentes aux

communications judiciaires (102). Mais est-ce (politiquement) possible ? Un vœu pieux ?

Notre propos s'est limité à un examen critique des textes. Encore faut-il bien entendu que les systèmes et solutions techniques retenus s'accordent à ceux-ci et donnent satisfaction sur le terrain, notamment en termes de fiabilité et convivialité. Qui vivra verra !

(102) Sont visés les multiples arrêtés royaux en préparation.